(12) UK Patent Application (19) GB (11) 2 346 239 (13) A

(43) Date of A Publication 02.08.2000

(21) Application No 0001092.6

(22) Date of Filing 19.01.2000

(30) Priority Data
(31) 09237387 (32) 26.01.1999 (33) US

(71) Applicant(s)
International Business Machines Corporation
(Incorporated in USA - New York)
Armonk, New York 10504, United States of America

(72) Inventor(s)
Thomas Yu-kiu Kwok
Lawrence S Mok

(74) Agent and/or Address for Service
R D Moss
IBM United Kingdom Limited, Intellectual Property
Department, Mail Point 110, Hursley Park,
WINCHESTER, Hampshire, SO21 2JN,
United Kingdom

(51) INT CL[7]
G07F 19/00 , G06F 1/00 12/14 , G07F 7/08

(52) UK CL (Edition R)
G4H HTG H1A H13D H14A H14B H14D
G4A AAP
U1S S2120 S2124 S2132

(56) Documents Cited
None

(58) Field of Search
UK CL (Edition R) G4A AAP , G4H HTG
INT CL[7] G06F , G07F
ONLINE:WPI,EPODOC,JAPIO

(54) Abstract Title
Card security and Web sites

(57) A method and system are disclosed for accessing personal Web site or executing electronic commerce securely in a smart Java card. A personal Web site which includes personal or private information is stored in a personal smart Java card. Before a user can access the Web site stored in the smart Java card, the user is validated by one or a combination of PIN, facial images, hand images, eye image, voice characteristics, and finger prints. Further, an encryption engine embedded in the smart Java card decodes and compares the entered PIN combined with a secure key or security certificate to verify the user's identity. Before the bank account can be accessed freely by the user, the bank's computer system checks the combined secure data to ensure the authenticity of the card and the user's identity with multiple check points using Internet security protocols via Web browses.

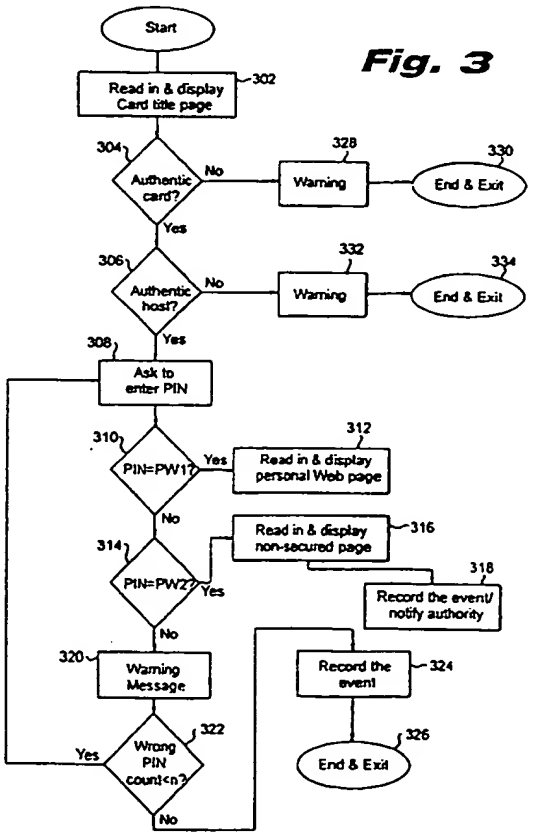

Fig. 3

GB 2 346 239 A

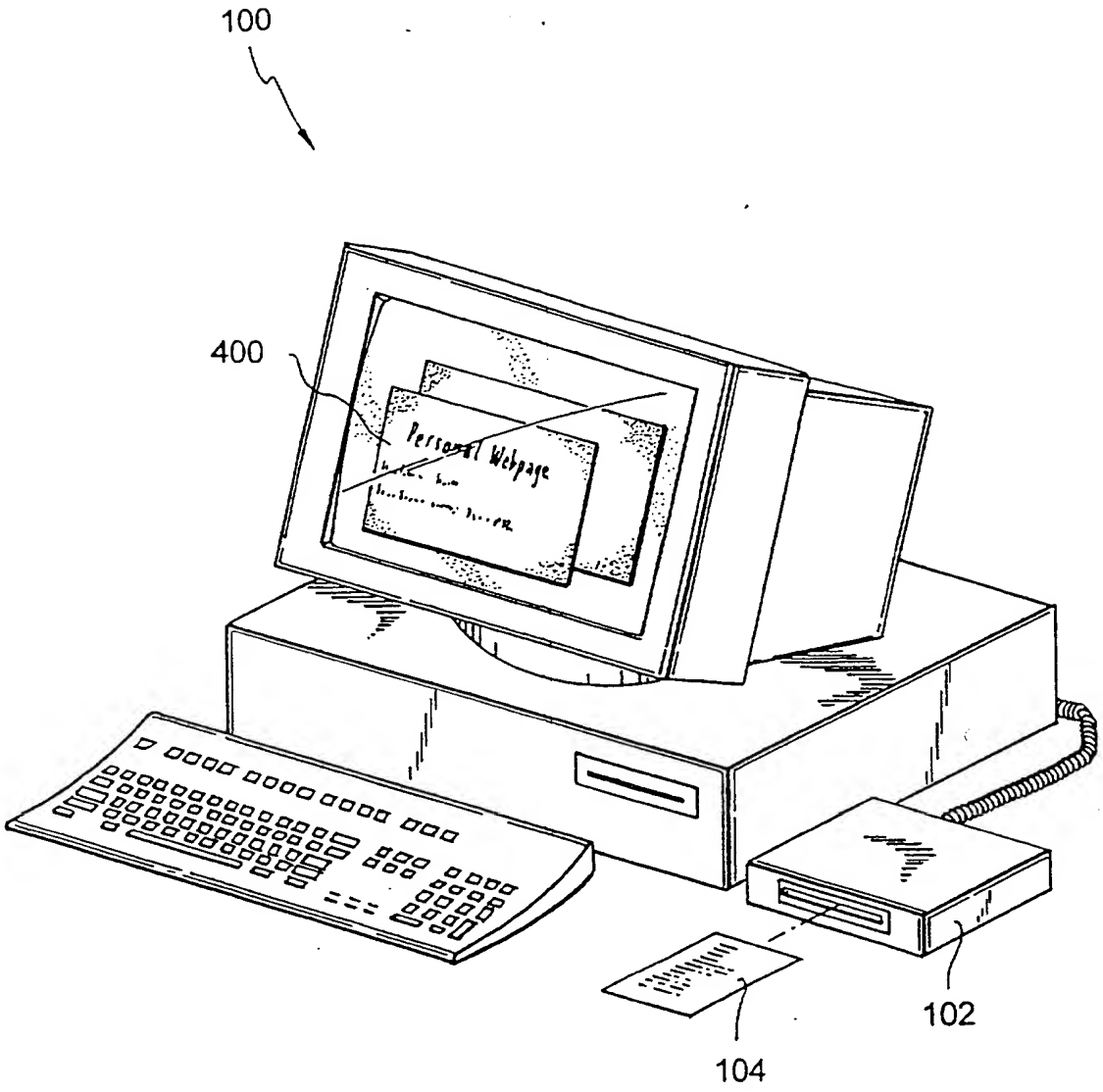

Fig. 1

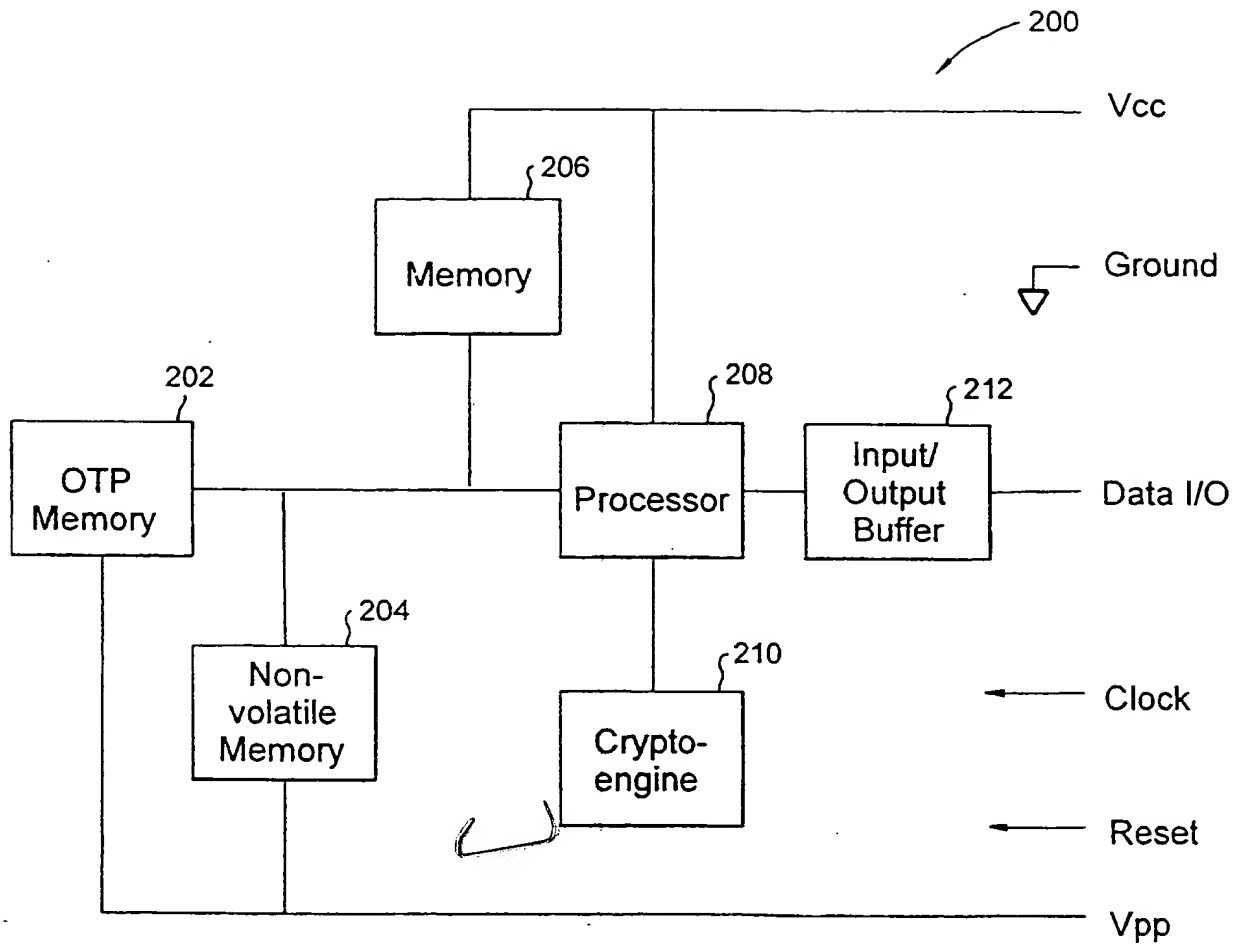

Fig. 2

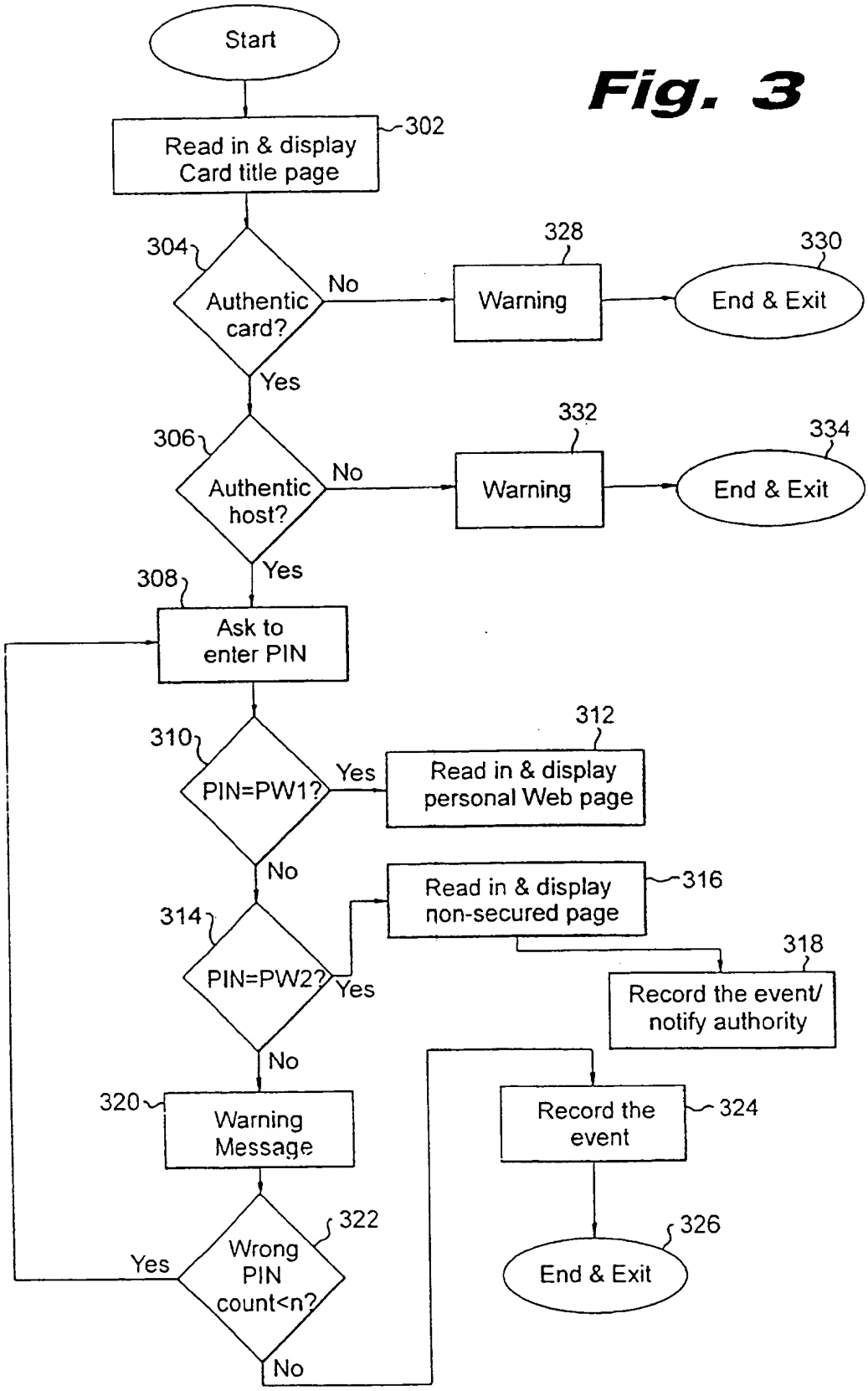

Fig. 3

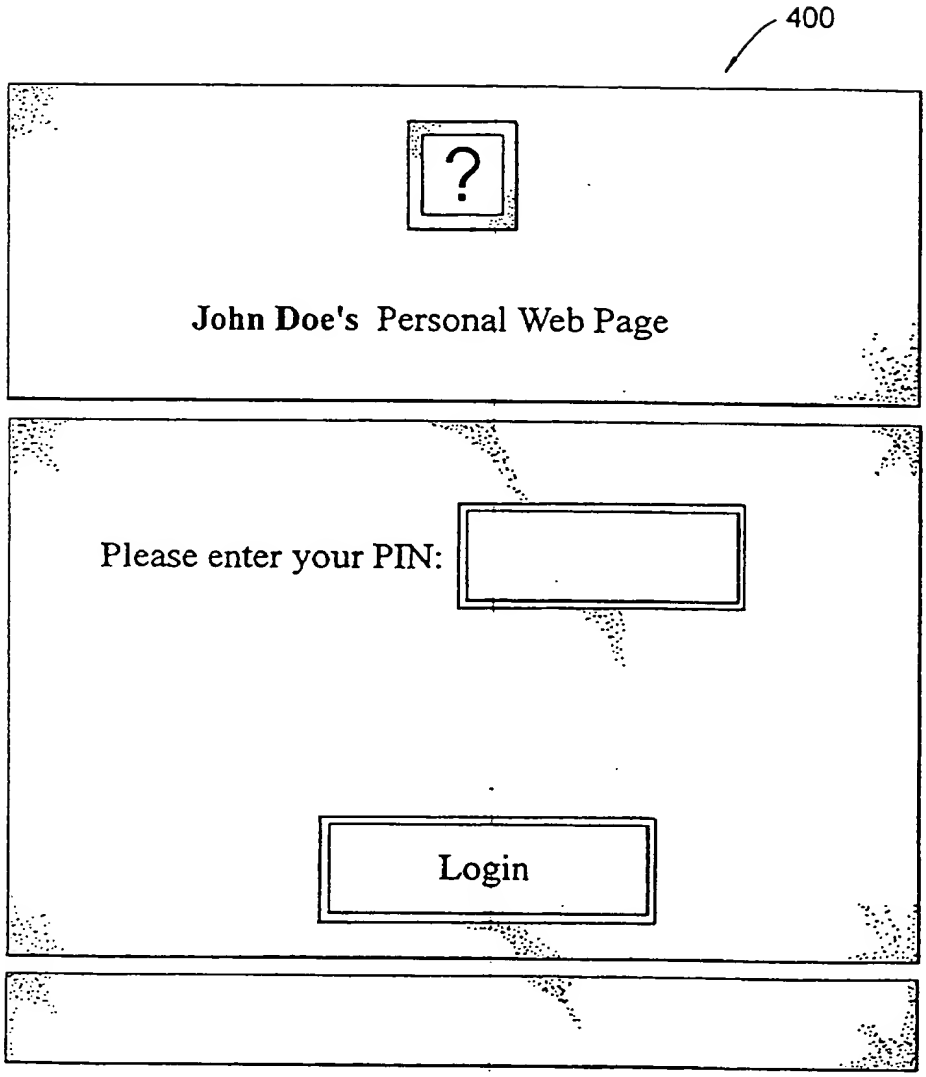

Fig. 4

A PERSONAL WEBSITE FOR ELECTRONIC COMMERCE ON A SMART JAVA CARD WITH MULTIPLE SECURITY CHECK POINTS

This invention relates to the electronic commerce on the Internet using a smart card and, in particular, to methods and systems for accessing and retrieving information from a personal web site stored in a smart Java card with security.

A smart card typically includes a plastic carrier, in which is embedded a specially designed integrated circuit (IC) and either a set of contacts or an aerial for the contactless operation. It contains at least one of three types of memories (ROM, RAM, and EEPROM) and/or a microprocessor. A smart card also needs to conform to the ISO 7810-7813 (bank card size and thickness), ISO 7816, EMV, ETSI standards. The most important aspect of the smart card is the ability to control the access to the card's memory by the use of password protection and/or other security mechanisms. Other important components of the system incorporating a smart card include the smart card reading devices and computer systems which access the information on the card during operation, and the systems which manufacture, issue, and control the smart card and the various encoding keys contained in the card.

A typical implementation of data security in computer systems involves providing a mechanism for proving the identity of the person sending or receiving messages and assuring that the message contents have not been altered. That is, confidentiality, authentication, integrity and non-repudiation are four modern data communications security requirements. These requirements can all be managed by using a form of cryptology. Cryptology, as well known by the persons skilled in the art, is a science of codes and ciphers. In cryptology, original data or plaintext is encrypted using a key. The encrypted data, or ciphertext, usually appears to be a meaningless series of bits which cannot be understood by anyone reading it. To restore the data into a readable text, the receiving person must decrypt the encrypted data. A typical encryption technique includes two main components: an algorithm, and a key. The same or a different algorithm/key pair may be employed by a decryption technique for decoding the encrypted data back to a readable text. Before the data is encrypted, the data is often scrambled or rearranged for further security. Encryption techniques are also used in digital signatures to authenticate the signing party.

Presently, smart cards are used throughout the industrialized countries to identify, to travel, to gain access to buildings, to obtain cash from the bank, to place telephone calls, and to pay for goods and services. Many governments use smart cards to pay welfare, medical, family and social benefits. The cards which are prevalent in daily applications usually have a memory governed by a type of fixed logic, but typically do not include a microprocessor.

Java is the object-oriented computer language that makes programming and distributing software easier and more secure because programs written in Java language are platform independent and have built-in security. Because the leading smart card manufacturers are developing smart cards with common operating system based on the Java Card API, the smart Java cards will become interoperable in almost any computer system. An application included in the smart Java card can be subsequently modified or updated with ease and convenience by a user. Moreover, the smart Java cards are not limited to having one application. Constrained only by a memory capacity, the smart Java cards can hold more than one application per card.

The widespread availability of World Wide Web (WWW or Web) phones, Personal Data Assistants (PDAs), and Windows-based CE machines with Internet connectivity provides anyone within reach of those devices a world wide access to the Internet. With such a wide access to the Internet, it is highly desirable to have efficient techniques for accessing the Web pages. An Internet user typically employs a browser to access the Web pages. The most popular browsers currently in use are Netscape's Navigator and Microsoft's Internet Explorer. Storing personal data in the Web page format in a smart Java card will make the card, hence the data, accessible almost everywhere and anytime with built-in security.

The following are some of the articles describing the current state of Smart cards. An article in the University of Maryland Website, http://des.umd.edu/~melody/research/smart_card.html, entitled "The Smart Card: Just How Smart Is It?" lists a variety of current applications of smart cards, for instance, toll payment, personal identification, health care, retail, and travel. With the advent of the Java language, a smart card can be programmed in Java, and hence, referred sometimes as Java

cards. A paper in the IEEE Internet Computing, Vol.1, no.1, pp. 57-59, Jan.-Feb. 1997, "Java Card: Internet Computing on a Smart Card", describes a scenario of using a smart card as a means to generate and store a private encryption key. As in the Schlumberger press release dated March 13, 1997, "Smart Cards to Catalyse 'Electronic-Commerce Explosion'", the company has developed a set of software tools that enables a secure Internet commerce and a smart card equipped with a Motorola chip that can perform public key encryption and decryption on the card. U.S. Patent 5,590,197, entitled "Electronic Payment System and Method", describes an electronic payment system in the form of an electronic wallet (smart card is one of the electronic forms) that contains protected account information and a file with a set of public keys stored in for encryption has been described.

The present invention accordingly provides, in a first aspect, a method for enabling multiple security check points during electronic transactions with a smart card, the smart card having one or more Web pages stored therein, the method comprising: checking authenticity of the smart card; verifying authenticity of a computer processing the smart card; receiving verification data from a user to identify the authenticity of the user; and displaying said one or more Web pages.

In a method of the first aspect, the step of displaying preferably includes displaying said one or more Web pages having personal secure information associated with the user.

In a method of the first aspect the step of displaying preferably includes displaying said one or more Web pages having a link to one or more second Web sites, said one or more second Webs site accessible over a computer network.

In a method of the first aspect the method preferably further includes: accessing said one or more second Web sites from said one or more Web pages; and automatically providing security data required for accessing said one or more second Web sites from said one or more Web pages.

In a method of the first aspect, the step of displaying preferably includes displaying said one or more Web pages having a link to one or

more second Web sites, said one or more second Web sites for processing electronic transactions over a computer network.

In a method of the first aspect, the step of displaying preferably includes displaying said one or more Web pages having a link to one or more second Web sites accessible over a computer network, said one or more second Web sites having additional personal secure information associated with the user.

In a method of the first aspect the step of receiving verification data preferably includes receiving any one of personal identification number (PIN), image data relating to physical attributes of the user, finger print data relating to the user, and voice characteristics relating to the user, or any combination thereof, the verification data used to verify user identity.

In a method of the first aspect, the step of checking authenticity of the smart card preferably includes validating a digital signature stored in the smart card.

In a method of the first aspect, the step of verifying authenticity of a computer preferably includes: receiving a security key generated using a public key; decrypting the security key with a private key; and determining whether the computer is authentic.

In a method of the first aspect, the step of receiving verification data preferably includes receiving a secondary PIN and the step of displaying includes displaying a Web page having non-secure information.

In a method of the first aspect, the method preferably further includes: sending data signals to a law enforcement authority for apprising the law enforcement authority of an emergency situation when the secondary PIN is received from the user.

In a method of the first aspect, the method preferably further includes: decoding by using said PIN, a stored secure key associated with a remote account server accessible over a computer network, before accessing the remote account server. The method preferably further includes the remote account server validating the secure key combined

with said PIN before allowing electronic transactions to be performed with the remote account server.

A method of the first aspect preferably further includes: encrypting secure contents of said one or more Web pages stored in the smart card when the smart card is not being used; and decrypting the secure contents before the step of checking the authenticity of the smart card.

A method of the first aspect preferably further includes: initiating a communication with the computer when the smart card is inserted into a card reading device; and invoking a Web browser in the computer for processing said one or more Web pages stored in the smart card.

A method of the first aspect preferably further includes: recording in a one-time-programmable memory, the memory embedded in the smart card, selected events processed with the smart card.

In a second and third aspect, the present invention provides, respectively, a system and a program storage device for performing steps of the method of the first aspect.

In a preferred embodiment of the present invention, a user's identity is first verified by the user's unique PIN (Personal Identification Number), optionally accompanied with images of the user's face, hand, and/or eye images. Additional checking of the user's identity in this first step may be performed using the user's voice characteristics and/or finger prints, before enabling the user to access to his or her personal Web site stored in the smart Java card.

Second, a secure key or security certificate, downloaded previously from the card issuer or a bank or financial institution, is stored in the smart Java card. The secure key or security certificate is sent to the host computer or bank ATM when the smart Java card is inserted into the reader. The key or certificate is then combined with the user entered PIN. The combined data is sent back to the smart Java card. The encryption engine in the card decodes the combined data to recover the PIN which is then compared with the authentic PIN stored in the card. If the PIN is correct, the secure personal Web page is sent to the host

computer. Similarly, a bank or a financial institution may verify the authenticity of the card and the user's identity whenever the user tries to electronically access the data associated with the financial institution through the Web browsers.

The methods and systems of this invention are particularly useful for authorized access to personal links, such as bank accounts, because the smart Java card has a capacity to store personal keys. Moreover, the smart Java card includes an encryption engine which manipulates the personal keys with other required user inputs to verify and authenticate the identity of the user. With the secure information and the encryption engine stored in the smart Java card, the present invention provides for security verifications at multiple check points, allowing the user to conduct electronic transactions including electronic commerce with improved security.

Further features and advantages of the present invention as well as the structure and operation of various embodiments of the present invention are described in detail below with reference to the accompanying drawings. In the drawings, like reference numbers indicate identical or functionally similar elements.

Preferred embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Fig. 1 is a schematic diagram showing the personal computer equipped with a card reader which accesses the smart Java card of the present invention;

Fig. 2 is the block diagram of the semiconductor chip embedded inside the smart Java card of the present invention with additional One-Time-Programmable memory;

Fig. 3 is the flow chart illustrating the multiple security check procedure of the smart Java card of the present invention; and

Fig. 4 is an example of a screen image showing an initial personal Web page stored in the smart Java card of the present invention.

The present invention is directed to a method and system for accessing a personal Web site stored in a smart Java card. The Web site can include, inter alia, security information such as personal identification numbers needed to access various financial accounts, and information needed to check and activate credit cards charges, for example, used in electronic commerce. In the preferred embodiment of the present invention, a personal Web site including personal or private information is stored in a personal smart Java card. Before a user can access the personal Web site, the private information, such as the PIN, user's facial images, finger prints, eye image, voice characteristics, are compared with those of the user's information previously stored in the smart Java card.

Furthermore, with information stored in a Web page on the smart Java card, additional Web sites whose Uniform Resource Locators (URLs) are typically encoded as hypertexts on a Web page can also be accessed via the Internet. Moreover, if these Web sites require an entry of security information before they can be accessed, the security information is automatically provided by the personal Web site stored in the smart Java card, without the user having to enter the information. For example, a password needed to access another Web site may be embedded in the Web page on the smart Java card. When the other Web site is accessed by using the URL, the password is automatically passed to the other Web site by for example, attaching it as a parameter with the URL, or by transmitting the password information as environment variables. By having the secure information including the passwords needed to access various Web sites over a computer network, e.g., the Internet, embedded in the Web page stored on the smart Java card, the user need not manually enter authentication information when accessing those sites electronically.

To provide additional layer of security check, the smart Java card may include a secure key or security certificate from each institution, e.g., banks, card issuer, credit card company, etc. When the user seeks an access to an account in any one of the institutions, an encryption engine in the smart Java card may combine the user entered PIN with the secure key associated with the institution. The combined secure data is then checked by the institution before the user can access the account via the Internet from the user's personal Web site stored in the smart Java card. Thus, the most important advantage of present invention is

the provision of multiple check points performed during various electronic transactions, including the electronic commerce.

In the preferred embodiment, the present invention includes three components. First, a personal Web site having personal and private information such as health records, financial data, link addresses to various accounts in banks or financial institutions and to other Web sites, is stored in his or her personal smart Java card. The personal Web page can generally be viewed by any commercially available Web browsers. Moreover, if the data becomes too large to be stored in the card memory, additional Internet link addresses to the outside Web site for storing the data are provided.

Second, for providing authorized access and secure updates to the personal Web site, the user's PIN, hand, facial and/or, eye images, voice characteristics and/or finger prints are optionally stored in the smart Java card. The card also stores the host authenticity code and includes an encryption engine for checking the authenticity of the host when the card's web page and stored data are being updated.

Third, additional passwords and personal keys used for accessing other Web sites including bank and financial institutions are also stored in the smart Java card.

The secure personal Web site in the smart Java card provides multiple check points for secure electronic commerce. For example, as an initial step, the user's PIN, facial, hand and/or eye images, voice characteristics, finger prints are verified allowing the user to access the Web site. Next, An encryption engine in the smart Java card uses the entered PIN to decode a previously stored secure key or security certificate associated with a Web site, such as a site for a financial institution. Before the user can access the Web site of the financial institution and, for example, the user's bank account at that financial institution, a Web server at that Web site would authenticate the user once again by checking the combined data in the smart Java card to insure the proper identity of the user.

Figure 3 illustrates the typical procedure of accessing the personal Web page stored in a smart Java card. Figure 1 illustrates a typical computer 100 having a smart card reader 102 connected to the

computer 100. When the card 104 is inserted into a card reader connected to a personal computer 100 as shown in Figure 1, or a bank ATM, the title page of the personal Web site is first displayed through an Internet browser. Referring back to Figure 3 at step 302, a typical title page 400 as shown in Figure 4 is displayed. At step 304, the card's authenticity is first checked by the computer processing the smart Java card. If the card is determined not to be authentic, a warning message is displayed at step 328 and the system exits at step 330. Any procedure or protocol used in the Internet can be used to check the card's authenticity, including the digital signature procedure used in the public-key encryption scheme. At step 306. if the card is authentic, the card checks for the authenticity of the host computer using its in-card processor and crypto-engine 210 as shown in Figure 2. If the host computer is determined not to be authentic, a warning message is displayed at step 332 and the system exits at step 334. If both card and host are authentic, the identity of the card owner is checked. In the example shown at step 308 of Figure 3, a PIN number is requested. If the entered PIN number is correct at step 310, a personal Web page showing personal and secure information is displayed at step 312.

In the preferred embodiment of the present invention a secondary PIN entry procedure is provided for additional security. The smart Java card processor is equipped to handle a secondary PIN entry during emergency situations. When this secondary PIN is entered, the personal Web page which is normally displayed will not be displayed. Instead, a second Web page which imitates the personal Web page but does not include any secure information is displayed. Since this Web page does not store any secure information, none of the highly secure information which may be stored in the personal Web page can be compromised. In addition to displaying this sham Web page, the smart Java card processor can be programmed to send a signal to the host computer, i.e., the computer processing the smart Java card, to notify an appropriate authority such as a law enforcement authority. This is useful in a situation when the card owner is forced unwillingly to access the card. Thus, referring back to Figure 3, at step 314, when the secondary PIN is entered, a Web page having non-secure information is displayed at step 316, and at 318, appropriate notification is sent with the recording of the event. At step 320, if neither correct PIN nor secondary PIN were entered, a warning message is displayed. At step 322, a number of times the wrong PIN was entered is recorded. If the number does not exceed a

predetermined number, at step 308, a user is prompted to enter a PIN again. If the number exceeds the predetermined number of times, the event is recorded at step 324, and at step 326, the user is exited from the procedure.

The block diagram 200 illustrating one embodiment of an internal configuration for a smart Java card is shown in Figure 2. The configuration shown in Figure 2 includes an One-Time-Programmable (OTP) memory 202 which is used to store critical information for extended security checks. The information stored in the OTP memory 202 are not erasable by any methods. Such permanent storage of information is useful for storing information about the card's authenticity and for recording any attempts of unsuccessful entries of PIN. The latter can be an important information for law enforcement officials when investigating how and when the card has been tempered. Additionally, the smart Java card includes a conventional non-volatile 204 and volatile 206 memory for storing intermediary data used during processing. The processor 208 typically commands and controls data signals communicated to the smart Java card via the input/output buffer 212. The processor also controls the crypto-engine 210 whenever a security key needs to be coded or decoded as described above. The secure communication protocol between the card and the host may be any prevailing secure protocols used in the Internet including the Secure Socket Layer (SSL) or Secure HTTP (S-HTTP).

The personal Web site embedded inside a smart Java card may be carried around anywhere by a person in a wallet or a purse. The smart Java card has a Web page written by either conventional or Java language, which can be accessed by any Web browsers with proper authorization. All or part of the conventional Internet communication and security protocols may be used between the smart Java card and the host computer processing the card. The personal Web site can be accessed when the smart Java card is inserted into a smart Java card reader connected to a host computer, i.e., either a personal computer or a bank ATM. The host computer having a running Web browser may then view the personal Web page by keying in the Web address, e.g., the URL. Alternatively, the personal Web site can initiate a contact to the host Web browser when the smart card is inserted into the reader. When the host Web browser detects the personal Web page from the smart Java card, further communications can be started. Such communications would follow the smart card and the host authenticity checks as wells as the validity the person that uses the Web browser by

using PIN, encryption keys, security certificate, any/or passwords procedures as described above. The personal Web page is thus enabled to provide personal secret links, including a link to the card holder's bank account. Moreover, if the host computer processing the smart Java card, e.g., a bank's ATM machine, is equipped with a camera and a microphone in the vicinity of the card reader, the bank computer may additionally programmed to match the person's physical profiles as detected from the camera and/or the microphone in real time with those of the information stored in the smart Java card and/or the bank's own computer. Additional advantage with using the smart Java card to store secure information is that the card is off line when it is not inserted in a reader and therefore, more difficult to temper with by hackers or in case of spoofing. Moreover, the smart Java card of the present invention is easily adaptable by the community because it uses a widely available Internet communications and security protocols and is runnable on any platform having a Java-enabled browser or interpreter.

CLAIMS

1. A method for enabling multiple security check points during electronic transactions with a smart card, the smart card having one or more Web pages stored therein, the method comprising:

checking authenticity of the smart card;

verifying authenticity of a computer processing the smart card;

receiving verification data from a user to identify the authenticity of the user; and

displaying said one or more Web pages.

2. A method as claimed in claim 1, wherein the step of displaying includes displaying said one or more Web pages having personal secure information associated with the user.

3. A method as claimed in claim 1 or claim 2, wherein the step of displaying includes displaying said one or more Web pages having a link to one or more second Web sites, said one or more second Webs site accessible over a computer network.

4. A method as claimed in any of claims 1 to 3, wherein the method further includes:

accessing said one or more second Web sites from said one or more Web pages; and

automatically providing security data required for accessing said one or more second Web sites from said one or more Web pages.

5. A method as claimed in any preceding claim, wherein the step of displaying includes displaying said one or more Web pages having a link to one or more second Web sites, said one or more second Web sites for processing electronic transactions over a computer network.

6. A method as claimed in any preceding claim, wherein the step of displaying includes displaying said one or more Web pages having a link

to one or more second Web sites accessible over a computer network, said one or more second Web sites having additional personal secure information associated with the user.

7. A method as claimed in any preceding claim, wherein the step of receiving verification data includes receiving any one of personal identification number (PIN), image data relating to physical attributes of the user, finger print data relating to the user, and voice characteristics relating to the user, or any combination thereof, the verification data used to verify user identity.

8. A method as claimed in any preceding claim, wherein the step of checking authenticity of the smart card includes validating a digital signature stored in the smart card.

9. A method as claimed in any preceding claim, wherein the step of verifying authenticity of a computer includes:

receiving a security key generated using a public key;

decrypting the security key with a private key; and

determining whether the computer is authentic.

10. A method as claimed in any preceding claim, wherein the step of receiving verification data includes receiving a secondary PIN and the step of displaying includes displaying a Web page having non-secure information.

11. A method as claimed in any preceding claim, wherein the method further includes:

sending data signals to a law enforcement authority for apprising the law enforcement authority of an emergency situation when the secondary PIN is received from the user.

12. A method as claimed in any of claims 4 to 11, wherein the method further includes:

decoding by using said PIN, a stored secure key associated with a remote account server accessible over a computer network, before accessing the remote account server.

13. A method as claimed in claim 12, wherein the method further includes the remote account server validating the secure key combined with said PIN before allowing electronic transactions to be performed with the remote account server.

14. A method as claimed in any preceding claim, wherein the method further includes:

encrypting secure contents of said one or more Web pages stored in the smart card when the smart card in not being used; and

decrypting the secure contents before the step of checking the authenticity of the smart card.

15. A method as claimed in any preceding claim, wherein the method further includes:

initiating a communication with the computer when the smart card is inserted into a card reading device; and

invoking a Web browse in the computer for processing said one or more Web pages stored in the smart card.

16. A method as claimed in any preceding claim, wherein the method further includes:

recording in a one-time-programmable memory, the memory embedded in the smart card, selected events processed with the smart card.

17. A system for processing a personal Web site stored in a smart card, the system comprising:

a smart card for storing one or more Web pages with personal secure data associated with a user;

a smart card reader device for reading and writing data from and to the smart card;

a computer connected to the smart card reader device, the computer further including a Web browse for accessing the personal secure data embedded in said one or more Web pages.

18. A system as claimed in claim 17, wherein said one or more Web pages include links to second one or more Web sites accessible over a computer network.

19. The system as claimed in claim 17 or claim 18, wherein the smart card further includes:

an encryption engine for encrypting and decrypting data with secure keys stored in the smart card; and

a processor which receives data generated by the encryption engine data for use in authenticating before any one of said one or more Web pages and one or more second Web sites are accessed.

20. The system as claimed in any of claims 17 to 19, wherein the smart card further includes:

a one-time-programmable memory whose contents cannot be erased, the one-time-programmable memory for storing secure data.

21. The system as claimed in claim 20, wherein the one-time-programmable memory further stores selected events processed by the smart card.

22. The system as claimed in any of claims 17 to 21, where said one or more Web pages include platform-independent computer instructions executable by any computer platform.

23. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for enabling multiple security check points during electronic transactions with a smart card, the smart card having one or more Web pages stored therein, the method steps comprising:

checking authenticity of the smart card;

verifying authenticity of a computer processing the smart card;

receiving verification data from a user to identify the authenticity of the user; and

displaying said one or more Web pages.

24. A program storage device as claimed in claim 23, wherein the method step of displaying further includes displaying said one or more Web pages having personal secure information associated with the user.

25. A program storage device as claimed in claim 23 or claim 24, wherein the method step of displaying further includes displaying said one or more Web pages having a link to one or more second Web sites, said one or more second Web sites accessible over a computer network.

26. A program storage device as claimed in any of claims 23 to 25, wherein the method steps further include:

accessing said one or more second Web sites from said one or more Web pages; and

automatically providing security data required for accessing said one or more second Web sites from said one or more Web pages.

27. A program storage device as claimed in any of claims 23 to 26, wherein the method step of displaying further includes displaying said one or more Web pages having a link to one or more second Web sites, said one or more second Web sites for processing electronic transactions over a computer network.

28. A program storage device as claimed in any of claims 23 to 27, wherein the method step of displaying further includes displaying said one or more Web pages having a link to one or more second Web sites accessible over a computer network, said one or more second Web sites having additional personal secure information associated with the user.

29. A program storage device as claimed in any of claims 23 to 28, wherein the method step of receiving verification data includes receiving any one of personal identification number (PIN), image data relating to physical attributes of the user, finger print data relating to the user, and voice characteristics relating to the user, or any combination thereof.

30. A program storage device as claimed in any of claims 23 to 29, wherein the method step of checking authenticity of the smart card includes validating an authorisation key stored in the smart card by decrypting with a private encryption key.

31. A program storage device as claimed in any of claims 23 to 30, wherein the method step of receiving verification data includes receiving a secondary PIN and the step of displaying includes displaying a Web page having none-secure information.

32. A program storage device as claimed in any of claims 23 to 31, wherein the method steps further include:

sending data signals to a law enforcement authority for notifying the law enforcement authority of an emergency situation when the secondary PIN is received from the user.

33. A program storage device as claimed in any of claims 29 to 32, wherein the method steps further include:

decoding by using said PIN, a stored secure key associated with a remote account server accessible over a computer network, before accessing the remote account server.

34. A program storage device as claimed in claim 33, wherein the method steps further include the remote account server validating the secure key combined with said PIN before allowing electronic transactions to be performed with the remote account server.

35. A program storage device as claimed in any of claims 23 to 34, wherein the method steps further include:

initiating a communication with the computer when the smart card is inserted into a card reading device; and

invoking a Web browse in the computer for processing said one or more Web pages stored in the smart card.

36. A program storage device as claimed in any of claims 23 to 35, wherein the method steps further include:

recording in a one-time-programmable memory, the memory embedded in the smart card, selected events processed with the smart card.

The Patent Office

INVESTOR IN PEOPLE

Application No:	GB 0001092.6	**Examiner:**	Mike Davis
Claims searched:	1-36	**Date of search:**	10 April 2000

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.R): G4H (HTG), G4A (AAP)

Int Cl (Ed.7): G07F, G06F

Other: Online: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
	None	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.